UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/182,279	10/29/1998	DON COPPERSMITH	YO998-313	1845

30743 7590 06/18/2003

WHITHAM, CURTIS & CHRISTOFFERSON, P.C.
11491 SUNSET HILLS ROAD
SUITE 340
RESTON, VA 20190

EXAMINER
NGUYEN, CUONG H

ART UNIT	PAPER NUMBER
3625	

DATE MAILED: 06/18/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.	Applicant(s)
09/182,279	Coppersmith et al.
Examiner	**Art Unit**
Cuong H. Nguyen	3625

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *Mar 31, 2003*.

2a) ☒ This action is **FINAL.** 2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-13 and 15-21* is/are pending in the application.

4a) Of the above, claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-13 and 15-21* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13) ☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

a) ☐ All b) ☐ Some* c) ☐ None of:

1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

*See the attached detailed Office action for a list of the certified copies not received.

14) ☒ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

15) ☒ Notice of References Cited (PTO-892)

16) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

17) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s). _____

18) ☐ Interview Summary (PTO-413) Paper No(s). _____

19) ☐ Notice of Informal Patent Application (PTO-152)

20) ☐ Other:

DETAILED ACTION

1. This Office Action is the answer to the communication received on 3/31/2003, which paper has been placed of record in the file.

2. Claims **1-13, 15-21** are pending in this application.

Response

3. The examiner withdraws the previous double-patenting rejections. Applicants' arguments have been fully considered but they are not persuasive with previous cited references for 35 U.S.C.§103(a) rejections. The examiner reviewed thoroughly the cited prior art again and he recognizes that those cited references are obvious with what the applicants claimed.

4. These following pertinent references have the same subject matter with the pending application; specifically the references of Goldman, and Berson were told to Mr. Michael Witham on 6/2003 (Mr. C. Lamont Whitham was not available). Mr. Michael Witham gave these pertinent references to IBM Corp. for further reviews.

- **Goldman**, (US Pat. 4,785,290 – 11/15/1988), Non-counterfeit able document system, wherein a system comprises a cryptographically encoded tag (T) having encoded information on the tag for verification. This encoded information are compared with signals from a database; hence, that tag is used as an identification means in shelf life and sales channels.
- **Bellare** et al., (US Pat. 5,673,318 – 9/30/1997), Method and apparatus for data authentication in a data communication environment; this invention teaches a receiving component generates a second tag which can then be compared with the transmitted tag to determine message authentication (determining an authentication tag).

- **Berson**, (US Pat. 5,768,384 – 6/16/1998), System for identifying authenticating and tracking manufactured articles; wherein a tag encrypted information is affixed to the manufactured article; a data center coupled to the manufacturing meters and located at a site remote from the manufacturing meters; means for producing information that identifies the manufactured articles; and a plurality of means located where the authenticity of the manufactured articles are checked by comparing the encrypted information on the article with the information produced that identifies the article.

- **Carlson**'s patent was cited because the applicants argue that "private/public keys, or encryption technique or de-crypt ion technique" were not disclosed in previous cited references .

5. Since the examiner is examining utility patents, the claims must be directed to systems, methods or articles of manufacture that have a clear utility. See MPEP 706.03(a) for example. Over the years, numerous court decisions have analyzed the content of various claimed language for meaningful, useful differences in structure or acts performed between the claims and the prior art. Some of these decision have found that certain language adds little, if anything, to the claimed structure or acts and thus do not serve as a limitation on the claims to distinguish over the prior art. For example, language directed to an intended use for a system in claim 1 did not result much in a structural or functional difference with respect to prior art for "electronically verifying authenticity" comprising "verifying data in a tag" and were held not to serve as a limitation on the claim. See in re **Schreiber**, 44 USPQ2d 1429 (CAFC 1997).

6. The examiner is unpersuasive with claimed concept of protecting goods against counterfeiting using smart tags that the applicants presented. The examiner submits that the use of smart cards, (or electronic tags - a derivative of smart cards) is obvious for one with skill in the art, it contains many different information because it has a memory chip, including routing information (see attached references of **Finast**, or **Bank Marketing Magazine**, or Retail Automation, or **Laurie Petersen**; see also the article title "Metrorail to take a high-tech trip with smart card" by the Washington Post, printed on 7/05/1998; it provides some background for a technology of using smart card). This article said that: "Smart cards -- which have been around for years in Europe", and (for the reader) "to known how many riders it has, but also who they are, where they get on the subway, where they go, and even what they have for lunch", and "Embedded in the card is a small computer chip that stores data. When the card is passed over the gate's reader, its antenna sends a signal to the gate to open. Computer chip: Holds approximately 30 times the data that can be stored on a magnetic-stripe card", and "Card reader: Rider passes card in front of the machine's reader to begin a transaction and again at the end of the transaction to register any changes", and "Non-contact smart card reader: Card is passed within three inches of reader. Riders can pass their entire wallet or purse over the disk. Display window shows how much is on the card", these information suggest an obvious use of smart card/smart tags/electronic tags in reading the information contained inside those cards/tags; from there, a purpose of protecting goods against counterfeiting is analogously achievable.

7. The examiner submits that **Fuji** clearly identifies GemPlus as a company that in a business of manufacturing, at least, and GemPlus' product obviously having analogous limitations as applicants claimed about GemPlus's electronic tags using in retailed business (**Fuji**'s article obviously suggest about smart/electronic tags using in retailed stores (see FUJI-KEIZAI USA, INC. pg.1, e.g. electronic tags, and GPR400, a smart card reader in PC Card format to instantly encrypt and decrypt reading data). Applicants argue that: "the article does not teach or suggest attaching a smart card to a product or goods such the authenticity of the good can be readily verified", the examiner submits that the concept of using smart card for authenticity/(getting secure/correct information), the suggestion of attaching a electronic tag/(smart card) to a product for a purpose is just an intend of use. The smart card/electronic tag, itself, **contains secured information** to trace/authenticate, among other things, original sources.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office Action:

> *(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

8. Claims **1, 5-6, 8-10, 15** are rejected under 35 U.S.C.§ 103(a) as being unpatentable over an article of **FUJI-KEIZAI** USA, INC., in view of **Carlson** et al. (US Pat. 4,758,714).

A. Referring to claim 1: It is directed to a system for verifying an authenticity of a product, comprising:

- a tag is attached to a product, it can store authentication information in encrypted form; and a reader equipped with a decryption key for reading said authentication information from said tag (to verify said product is authentic).

In page 5, para.2 of the argument received on 2/27/2002, the applicant admits that "The Fuji-Kezai reference describes the use of a smart card with encrypted data. However, it can be seen that the article deals only with data storage and retrieval concept". The examiner submits that this reference suggests MORE THAN what is showed. Although, it does not expressly show the intend of use of such smart tags, artisan would appreciate WHY these smart tags were manufactured, and WHERE these smart tags would be placed. These are intend of use, this reference doesn't need to disclose that information.

The above limitations are obviously included in GEMPLUS product (see FUJI-KEIZAI USA, INC. pg.1, e.g. electronic tags, and GPR400, a smart card reader in PC Card format to instantly encrypt and decrypt reading data);(see also Chew (US. Pat. 5,901,303) suggests a similar application (e.g. a tag having a memory) with a microprocessor embedded in a smart card).

Carlson et al. also disclose that public/private keys, encryption/de-cryption techniques at point-of-sales have been used. They also disclose that a verification step is done and routing information was used for satisfactorily verification. (**Carson** et al.'s patent discloses that: "This invention anticipates the use of checks as they currently exist using the Fed MICA system. However, a modified check may be used in the future which is a standard check save for the addition of an "NCR" (no carbon required) slip on the back entitled D-8 and a mag-stripe adhered to the front labeled D-17/D-18 shown in FIG. 11. The NCR page would include the amount of the check, D-16 and the serial number of the

check D-15 as well as the company's logo and other regulated information. It may or may not include the duplication of the payer's signature and countersignature, D-11 and D-13. However, it would naturally reproduce the Payee's name, D-12 and the date, D-14. D-11 and D-13 could possibly be obscured by a vision blocking ink screen such as seen on common personal checks with NCR pages. However, a preferred method to handle personal checks, Gov't checks, Travelers checks or any negotiable instrument using the Fed's MICA system would be to utilize the optional "dot matrix" or comparable type printer together with the optional alphanumeric keypad at 2-10 (15-10 and 14-10) and the onboard CPU' s and verification circuitry to automatically contact the issuer's bank computer, electronically transfer the required funds directly to the payee's bank account ("electronic funds transfer" also known as "EFT") and then cancel the check or instrument in the device all at the point-of-sale. This would be accomplished in much the same way as EFT is used with bank credit cards today. Those skilled in the art will readily recognize that this method is preferred should applicable laws allow. The scenario of the EFT/POS-CANCELLATION will be as follows: Mr. XYZ is out of town and wants to make a purchase at a stranger's establishment. He would present his check, already filled out in full as per customary procedures. The retailer would punch in the check amount at 2-10 which would read out at 2-23 for the retailer and the customer to see and then place the check in the device and close the 1-2 lid. The customer would then enter his personal identification number at the PIN keypad. It should be noted here that the machine will only take a PIN entry a certain number of second before the 1-2 lid is closed and will accept a PIN entry only a certain number of second after the 1-2 lid is closed. This is to help prevent a "residual" PI entry from incorrectly hindering a legitimate sale and enhance the security of the device. When the 1-2 lid closes the device's CPU

(which may or may not contain the customer's PIN entry at this time) will trigger the function of the MICA read head assembly to "read" the data on the check. If a mag-stripe is located on the check, it will also read that information. The CPU will then compare the PIN entered by the customer to that interpolated from the MICA information. This interpolation process may utilize the onboard algorithm modules in the module drawer or may depend upon outboard interpolation. Outboard interpolation would allow each bank to solely hold their own encryption /decryption methods and algorithm thus maintaining a higher state of security. Returning to the scenario; if the onboard CPU cannot interpret the PIN match up, then it would automatically call up the MICA network and using the routing and transit numbers on the face of the check would locate the very bank this particular check issued from. The MICA information sent from the onboard CPU would enter the bank's computer via suitable circuitry whereupon the bank's computer would use the encryption/decryption methods and/or algorithms known only to it to make the PIN comparison. For example, the bank's computer may use a combination of routing and transit numbers, account numbers and even individual check numbers in conjunction with their own security algorithm (known only to this bank's computer and perhaps key personnel) to arrive at a PIN which would either match or not match with that entered by the customer at the point-of-sale. At an appropriate time, the bank's computer would be told the amount of the check and its individual number as supplied by the POS terminal, examine whether the customer's balance is sufficient to cover the check, receive the payee's bank number and account number, and if all functions are deemed desirable, the payer's bank computer would electronically transfer the funds and debit the payer's account. The payee's routing and transfer and bank numbers and the payee's account number would be transferred to the payer's bank computer only after a satisfactory PIN match had been made. It should be noted

that the POS device described herein can be programmed with the retailers (payee's) routing and transit numbers, bank numbers and account numbers quite easily via the 2-10 keypad by qualified personnel. Then, after the EFT had taken place, the payer's bank computer would wire the appropriate check cancellation information to the POS terminal which would then (A) print it on the back of the check via the dot matrix printer and (B) if the "daily totals" option is onboard, would add the amount of the EFT to the daily total. The 1-2 cover would then pop open and the cancelled check would be presented to the customer as part of his receipt. Thus, the banks are shifting much of their check handling to the point-of-sale".

In Detailed Description Text (para. 43), **Carson** et al.'s patent discloses that: "FIGS. 13 and 16 show an alternative design to that discussed so far in this section. This alternative design more readily accommodates traveler's checks, personal checks, food stamps, etc. and in fact constitutes refinement and improvement over that system shown in FIGS. 5 and 6. A MICA reader device, 14-76, 15-76, and 16-76, such as that in common use by the Federal Reserve Banking System is installed adjacent to the 13-36 (14-36 and 15-36) mag-stripe reader head. This is possible since the three mag-stripe tracks on common credit cards and the MICA line on all checks are in such close proximity as shown by Figure 15. Due to strict Standard's regulations, this phenomenon is likely to remain indefinitely. As has been previously stated, the selection of which "head" to use is automatically made prior to verifier movement by the system's CPU in association with the switches numbered 15-18, 15-18A and 15-86. The position of the MICA, PIN, or offset number on the 15-78 check is shown at 15-75A and will be read as a part of the routing and transit numbers and account numbers preceding it in the MICA line.".

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use a readily available information/system on the market from **GEMPLUS** with **Carlson**'s suggestion since it is well-known on this particular field of retail marketing, and it makes a similar compact system for verifying an authenticity of a product at POS.

B. Re. to claim **5**: It is quite obvious to one with skills in the art to further (with the rationale for rejection in claim 1) including a reader (for authenticating a product) in front of a consumer prior to purchase of the product (see In re **Larson**, 144 USPQ 347 (CCPA 1965) for about **integration** characteristic in claim).

C. Re. to claim **6**: It is quite obvious to one with skills in the art to further (with the rationale for rejection in claim 1) including a reader for reading an electronic tag without physically contacting said tag (see FUJI-KEIZAI USA, INC. pg.1, e.g. RF/ID products from GEMPLUS do not need physically contacting a tag for reading information).

D. Re. to claim **8**: It is very well-known to one with skills in the art to further (with the rationale for rejection in claim 1) imply that authenticating product information is directed to a product 's manufacturer (e.g. a company names "Sony").

E. Re. to claim **9**: It is very well-known to one with skills in the art to further (with the rationale for rejection in claim 1) indicate that authentication information is specific to a product (e.g. a product serial number).

F. Re. to claim **10**: It is very well-known to one with skills in the art to further (with the rationale for rejection in claim 1) including a label having authentication information printed thereon to be verified against the authentication information read by a reader (e.g. a product serial number).

G. Re. to claim **18**: This claim has a similar limitation as claim 10 although it is a method claim; hence, the same rationale is incorporated.

H. Re. to claim **15**: It is obvious to one with skills in the art (with the rationale for rejection in claim 1) to have authentication information including information for authenticating an electronic tag (e.g. an analogous application is the BIOS file in a PC with information about a configuration of that PC -embedded information-.

In summary, the same analysis and reasoning set forth in the rejection of claim 1 are applied to these claims also because they are directed to a system that comprises similar means with very obvious limitations.

9. Claim **2** is directed to a system for verifying an authenticity of a product, wherein a tag is a smart card (see FUJI-KEIZAI USA, INC. pg.1, e.g. electronic tags, and GPR400, a smart card reader in PC Card format to instantly encrypt and decrypt reading data);(see also Chew (US. Pat. 5,901,303) suggests a similar application (e.g. a tag having a memory) with a microprocessor embedded in a smart card).

10. Claim **3** is directed to a system for verifying an authenticity of a product, wherein a tag is embedded into a product/(a product packaging) (e.g. see also Storch et al. (US Pat. 5,367,148) Figs. 2-3, the rationales for rejection for claim 1 are incorporated).

11. Claim **4** is rejected under 35 U.S.C. § 103 as being unpatentable over an article of FUJI-KEIZAI USA, INC., in view of **Mob** (US Pat. 5,740,250), and further in view of **Carlson** et al. (US Pat. 4,758,714).

It is directed to a system for verifying an authenticity of a product, wherein information is encrypted using a private key, and is decrypted using a public key (see **'250** claims 21, and 26; the rationales for rejection for claim 1 are incorporated herein).

It would have been obvious to one of ordinary skill in the art at the time of invention to implement the system of GEMPLUS with the suggestions of Mob for

verifying the authenticity of a product in a conventional way (as **Carlson's patent**), because these information were readily available at that time.

12. Claim **7** is rejected under 35 U.S.C. § 103 as being unpatentable over an article of FUJI-KEIZAI USA, INC., in view of **Guillou** et al. (US Pat. 5,140,634).

Claims **7** is directed to a system for verifying an authenticity of a product, wherein a zero-knowledge protocol is used (see at least **'634** the abstract, the rationales for rejection for claim 1 are incorporated herein).

It would have been obvious to one of ordinary skill in the art at the time of invention to implement the system of GEMPLUS with the suggestions of Guillou et al. for verifying the authenticity of a product, because these information are readily available at that time, and the verifying system would be done in a conventional way.

13. Re. to claim **17**: This claim has a similar limitation as claim 7 although it is a method claim; hence, the same rationale is incorporated for rejection.

14. Claim **11** is rejected under 35 U.S.C. § 103(a) as being unpatentable over an article of **FUJI-KEIZAI** USA, INC., in view of **Storch** et al. (US Pat. 5,367,148).

A system for verifying the authenticity comprises a product serial number.

The rationales for rejection for claim 1 are incorporated herein.

FUJI-KEIZAI INC.'s article do not expressly disclose above limitation.

However, **Storch** et al. show that this limitation is very well-known (see at least **'148** Fig. 3).

It would have been obvious to one of ordinary skill in the art at the time of invention to implement the system of GEMPLUS with the suggestions of Storch et al. 's disclosure for verifying the authenticity of a product serial number, because this information is very well-known, and the verifying system would be sufficient with a product's serial number.

15. Claim **12** is rejected under 35 U.S.C. § 103 as being unpatentable over an article of FUJI-KEIZAI USA, INC., since it is interpreted as: A system for verifying the authenticity comprises a graphical image/indicia (of the product) (this limitation is very well-known on the market, e.g. an apple for an "Apple computer" .etc., the rationales for rejection for claim 1 are incorporated herein).

16. Claims **13, 20** are rejected under 35 U.S.C.§ 103 as being unpatentable over an article of FUJI-KEIZAI USA, INC., in view of **DiCesare** et al. (US Pat. 5,971,435), and further in view of **Carlson** et al. (US Pat. 4,758,714).

A. Re. to claim 13: It is interpreted as a system for verifying the authenticity comprises an ownership history (of the product). The rationales for rejection for claim 1 are incorporated herein.

FUJI-KEIZAI USA, INC.'s article does not expressly disclose above limitation.

However, DiCesare et al. show that this limitation is very well-known (see '**435** 4:40-56, and claim 13) (together with **Carlson**'s disclosure).

It would have been obvious to one of ordinary skill in the art at the time of invention to implement the system of GEMPLUS with the suggestions of Carlson and DiCesare et al. 's disclosures for verifying the authenticity of a product, because these information are readily available at that time, and the verifying system would be sufficient with a product's past history.

B. Re. to claim **20**: This claim has a similar limitation as claim 13 although it is a method claim; hence, the same rationale is incorporated.

17. Claim **19** is rejected under 35 U.S.C. § 103 as being unpatentable over an article of FUJI-KEIZAI USA, INC., in view of Matyas et al. (US Pat. 5,164,988).

Re. to claim **19**: The rationales for rejection for claim 1 are incorporated herein.

It is interpreted as a system for verifying the authenticity, wherein (authentication) information is erased after being read.

FUJI-KEIZAI USA, INC.'s article does not expressly disclose above limitation.

However, **Matyas** et al. show that this limitation is very well-known (e.g. see **'988** 19:25-26, and 20:2-4).

It would have been obvious to one of ordinary skill in the art at the time of invention to implement Gemplus's system with a suggestion of Matyas et al. for verifying the authenticity of a product, because these information are readily available at that time, and the verifying task would be known as "done" with that product.

18. Referring to claims **16, 21**: They are rejected on obviousness reasons under 35 U.S.C. § 103(a) since limitations of these claims comprise similar claims' limitations of claims 1-15 above. The same analysis and reasoning set forth in the rejection of claims 1-15 are applied to these claims also because they are directed to a method that using similar means for verifying the authenticity of a product/(detecting products in a parallel market)(as the system in claims 1-15) to perform claimed steps.

19. Claim **21** is rejected under 35 U.S.C. § 103 as being unpatentable over an article of **FUJI-KEIZAI** USA, INC., in view of Matyas et al. (US Pat. 5,164,988), in view of **Carlson** et al. (US Pat. 4,758,714); and further in view of Dialog Classic article of "GE Capitol and GEMPLUS...".

Claim **21** is broad in its preamble because the only present concept of detecting counterfeit products in a market is derived from that claimed method. It has an feature that is different from above claims 1-20: **verifying a routing information of a product** (other modified clauses that are claimed for above step are obvious for one with skills in the art). Upon reviewing, above limitation

is obviously suggest with **GemPlus** smart tags because the tags contain a memory; therefore, routing information obviously must be written in a said memory "chip".

It would have been obvious to one of ordinary skill in the art at the time of invention to implement **GEMPLUS**'s system with a suggestion of **Carlson** et al., and **Matyas** et al. in Fuji-Kezai 's electronic tags for verifying the authenticity/information of a product, because these information/technologies are readily available at that time, and the verifying task would be obviously included for a product. Therefore, Claim 21 is rejected also based on obviousness reason.

Conclusion

20. Claims 1-13, 15-21 are rejected. THIS ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicants are reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

21. These references are considered pertinent to applicants' disclosure.

- FUJI-KEIZAI USA, INC., "Top 40 high tech companies in Europe: GEMPLUS, FRANCE: Analysis of factors/strategies for company's success, future plans and business opportunities in this industry", published on July 1997.

- Edelstone et al., "Microchip Technology - Company Report" by PRUDENTIAL SECURITIES INC., published on 11/24/1995.

- "GEMPLUS announces integration of GemSAFE with IBM Smart Card Security Kit" from Business Wire, p.1323, published on 10/21/1998.

- "GEMPLUS to showcase GemSAFE Smart Card Security Solutions at RSA Conference." from Business Wire, p.1418, published on 1/14/1999.

- Reid, article title "Metrorail to take a high-tech trip with smart card" by the Washington Post, printed on 7/05/1998; it provides some background for using smart card/electronic tag.

- **Goldman**, (US Pat. 4,785,290 – 11/15/1988), Non-counterfeitable document system, wherein a system comprises a cryptographically encoded tag (T) having encoded information on the tag for verification. This encoded information are compared with signals from a database; hence, that tag is used as an identification means in shelf life and sales channels.

- **Bellare** et al., (US Pat. 5,673,318 – 9/30/1997), Method and apparatus for data authentication in a data communication environment; this invention teaches a receiving component generates a second tag which can then be compared with the transmitted tag to determine message authentication (determining an authentication tag).

- Berson, (US Pat. 5,768,384 – 6/16/1998), System for identifying authenticating and tracking manufactured articles; wherein a tag encrypted information is affixed to the manufactured article; a data center coupled to the manufacturing meters and located at a site remote from the manufacturing meters; means for producing information

that identifies the manufactured articles; and a plurality of means located where the authenticity of the manufactured articles are checked by comparing the encrypted information on the article with the information produced that identifies the article.

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Cuong H. Nguyen whose telephone number is 703-305-4553 The examiner can normally be reached on Mon.-Fri. from 7:15 AM to 3:15 PM (EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ms. Wynn Coggins, can be reached on (703)308-1344.

Any response to this action should be mailed to:

Amendments

Commissioner of Patents and Trademarks
Washington D.C. 20231

or faxed to:
(703)305-7687 [Official communications]

or 703-746-5572 (RightFax)

Hand delivered responses should be brought to Crystal Park 5, 2451 Crystal Drive, Arlington, VA, 7th floor receptionist.

Receptionist: (703)308-1113.

Cuonghnguyen
Primary Examiner
June 15, 2003